Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Original) A method for preventing packet retransmissions during Internet Protocol security (IPsec) security association establishment comprising:

monitoring application socket requests;

requesting a Transmission Control Protocol (TCP) connection by an application;

determining if there is an active security association that exists to protect network flow associated with the connection request;

preventing the connection request from proceeding if no active security association exists to protect the network flow;

determining if a security policy exists for the network flow if no active security association exists to protect the network flow;

alerting a security association negotiation component to initiate negotiation for a security association based on the security policy if the security policy exists for the network flow; and

allowing the connection request to proceed if one of the active security association exists and the security association is established from the negotiation.

2. (Original) The method according to claim 1, wherein the security association negotiation component comprises an Internet Key Exchange (IKE) component.

3. (Original) The method according to claim 1, wherein the active security association and the security association are based on at least one of a source Internet Protocol (IP) address, a destination IP address, a protocol, a source port, and a destination port.

4. (Original) The method according to claim 3, wherein the protocol comprises one of TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP).

5. (Original) The method according to claim 1, further comprising determining if the network flow can be allowed without a security association if no security policy exists for the network flow.

6. (Original) The method according to claim 1, further comprising retrieving the security association from a database.

7. (Original) The method according to claim 6, wherein the database contains mappings between network flow information and security associations.

8. (Original) The method according to claim 7, wherein the network flow information comprises at least one of a source Internet Protocol (IP) address, a destination IP address, a protocol, a source port, and a destination port.

9. (Original) The method according to claim 1, further comprising retrieving the security policy from a database.

10. (Currently Amended) A method for preventing packet retransmissions during Internet Protocol security (IPsec) security association establishment comprising:

monitoring application socket requests;

requesting transmission of User Datagram Protocol (UDP) data on a socket by an [[the]] application;

determining if the socket has been associated with an active security association;

determining if there is a defined security association that may be used to protect network flow if the socket has not been associated with an active security association;

determining what security policy should be used when negotiating a security association for the network flow if there is no defined security association that may be used to protect the network flow;

preventing the UDP data from being sent if there is no defined security association that may be used to protect the network flow;

alerting a security association negotiation component to initiate negotiation for the security association if there is no defined security association that may be used to protect the network flow;

establishing the security association; and

allowing the UDP data to be sent in response to establishment of the security association.

11. (Original) The method according to claim 10, wherein the security association negotiation component comprises an Internet Key Exchange (IKE) component.

12. (Original) The method according to claim 10, comprising negotiating for a security association using security parameters specified by a policy.

13. (Original) The method according to claim 10, wherein the second determining comprises comparing filters with at least one of a source Internet Protocol (IP) address, a destination IP address, a protocol, a source port, and a destination port, the at least one of a source Internet Protocol (IP) address, a destination IP address, a protocol, a source port, and a destination port related to the network flow, the filters related to defined security associations.

14. (Original) The method according to claim 13, each filter comprising at least one of a source Internet Protocol (IP) address, a destination IP address, a protocol, a source port, and a destination port.

15. (Original) The method according to claim 13, wherein the security policy comprises at least one filter.

16. (Original) The method according to claim 10, further comprising determining if the network flow can be allowed without a security association if no security policy exists for the network flow.

17. (Original) A computing device for preventing packet retransmissions during Internet Protocol security (IPsec) security association establishment with a network unit, the device and network unit operably connected to a network, the computing device comprising:

a network interceptor, the network interceptor monitoring an application's socket requests;

a security association database operably connected to the network interceptor, the security association database containing a mapping of network flow information to security association information;

a security policy database operably connected to the network interceptor, the security policy database containing policies that describe parameters that are to be used in a negotiation of a security association;

a security association negotiation component, the security association negotiation component operably connected to the network interceptor, the security association negotiation component capable of negotiating a security association with a network unit; and

an Internet Protocol security (IPsec) packet classifier, the IPsec packet classifier responsible for performing IPsec processing on incoming and outgoing packets,

wherein the network interceptor insures that a security association is in place before allowing network traffic to flow between the application and the network unit.

18. (Original) The device according to claim 17, wherein the network flow information comprises at least one of Internet Protocol (IP) addresses, protocol, and ports.

19. (Original) The device according to claim 17, wherein the security association negotiation component comprises Internet Key Exchange (IKE).

20. (Original) An article comprising a storage medium having instructions stored therein, when executed causes a computing device to perform:

monitoring application socket requests;

requesting a Transmission Control Protocol (TCP) connection by an application;

determining if there is an active security association that exists to protect network flow associated with the connection request;

preventing the connection request from proceeding if no active security association exists to protect the network flow;

determining if a security policy exists for the network flow if no active security association exists to protect the network flow;

alerting a security association negotiation component to initiate negotiation for a security association based on the security policy if the security policy exists for the network flow; and

allowing the connection request to proceed if one of the active security association exists and the security association is established from the negotiation.

21. (Original) The article according to claim 20, wherein the security association negotiation component comprises an Internet Key Exchange (IKE) component.

22. (Original) The article according to claim 20, comprising negotiating for a security association using security parameters specified by a policy.

23. (Original) The article according to claim 20, wherein the active security association comprises at least one of source Internet Protocol (IP), destination IP, protocol, source port, and destination port.

24. (Currently Amended) An article comprising a storage medium having instructions stored therein, the instructions when executed causes a computing device to perform:

monitoring application socket requests;

requesting transmission of User Datagram Protocol (UDP) data on a socket by the application;

determining if the socket has been associated with an active security association;

determining if there is a defined security association that may be used to protect network flow if the socket has not been associated with an active security association;

determining what security policy should be used when negotiating a security association for the network flow if there is no defined security association that may be used to protect the network flow;

preventing the UDP data from being sent if there is no defined security association that may be used to protect the network flow;

alerting a security association negotiation component to initiate negotiation for the security association if there is no defined security association that may be used to protect the network flow;

establishing the security association; and

allowing the UDP data to be sent in response to establishment of the security association.

25. (Original) The article according to claim 24, wherein the security association negotiation component comprises an Internet Key Exchange (IKE) component.

26. (Original) The article according to claim 24, comprising negotiating for a security association using security parameters specified by a policy.

27. (Original) The article according to claim 24, wherein the active security association comprises at least one of source Internet Protocol (IP), destination IP, protocol, source port, and destination port.

28-29. (Canceled)